1.1. Grupos y subgrupos

- Se llama **Grupo** a un par $(G, *)$, donde G es un conjunto no vacío y $*$ es una operación interna en G que verifica:

  g_1 Propiedad **asociativa**: $(a * b) * c = a * (b * c)$ para todos $a, b, c \in G$

  g_2 Existe **elemento neutro**: $\exists\, e \in G$ tal que $e * a = a$ para todo $a \in G$.

  g_3 Existe **inverso u opuesto** de cada elemento: $\forall\, a \in G$ existe $a' \in G$ tal que $a' * a = e$.

- Se dice que que $(G, *)$ es un **grupo abeliano** si además se verifica:

  g_4 Propiedad **conmutativa**: $a * b = b * a$ para todos $a, b \in G$

- Ejemplos

Se llama **orden** del grupo $(G, *)$ al cardinal del conjunto G y se nota por $|G|$. Si $(G, *)$ es un grupo finito, la operación $*$ se puede describir mediante una tabla, denominada **Tabla de Cayley** del grupo.

Lemas

1. Si $*$ es una operación asociativa en G, entonces $(a * b) * (c * d) = (a * (b * c)) * d$
2. Sea $(G, *)$ es un grupo con elemento neutro e. Para todo $a \in G$ si $a * a = a \Rightarrow a = e$

Teorema 1: Inverso y neutro por la derecha

Sea $(G, *)$ un grupo con elemento neutro $e \in G$,

1. Para todos $a, a' \in G$ tales que $a' * a = e$ se verifica que $a * a' = e$
2. Para todo $a \in G$ se verifica que $a * e = a$

Teorema 2: Unicidad del neutro y del inverso

1. En todo grupo $(G, *)$ el elemento neutro es único
2. En todo grupo $(G, *)$ el inverso de cada elemento $a \in G$ es único.

Notaciones

Si no existe ambigüedad en la operación, el grupo $(G, *)$ se notará simplemente G.

Sean $a, b \in G$:

G	en un grupo general	en un grupo abeliano
operar a con b	$a * b$, ab	$a + b$
elemento neutro	e, 1	z, 0
potencia $0 \in \mathbb{Z}$ del elemento $a \in G$	$a^0 = e$	$0a = z$
potencia $1 \in \mathbb{Z}$ del elemento $a \in G$	$a^1 = a$	$1a = a$
potencia $n \in \mathbb{Z}$ para $n \geq 2$	$a^n = a * a^{n-1}$	$na = a + (n-1)a$
potencia $-1 \in \mathbb{Z}$ del elemento $a \in G$	$a^{-1} = a'$ **(inverso)**	$-a = a'$ **(opuesto)**
potencia $-n \in \mathbb{Z}$ para $n \geq 2$	$a^{-n} = (a^{-1})^n$	$(-n)a = n(-a)$

Propiedades cancelativas por la derecha y por la izquierda

- Sea $(G, *)$ un grupo, $\forall\, a, b, x \in G$ si $x * a = x * b$ entonces $a = b$
- Sea $(G, *)$ un grupo, $\forall\, a, b, x \in G$ si $a * x = b * x$ entonces $a = b$

Grupos de congruencias módulo n: $(\mathbb{Z}_n, +_n)$ y $(\mathbb{U}_n, \cdot_n)$

Dado $n \in \mathbb{N}$, se define en $\mathbb{Z}$ la relación de equivalencia **congruencia módulo** n:

$$a \equiv_n b \Leftrightarrow n|(b-a)$$

El conjunto cociente $\mathbb{Z}/\equiv_n$ se nota $\mathbb{Z}_n$ y para cada $a \in \mathbb{Z}$ su clase es $[a]_n = \{x \in \mathbb{Z} : x \equiv_n a\} \in \mathbb{Z}_n$.

1. En $\mathbb{Z}_n$ se define $[a]_n +_n [b]_n = [a+b]_n$. Se verifica que $(\mathbb{Z}_n, +_n)$ es un grupo abeliano.
2. Sea $\mathbb{U}_n = \{[r]_n \in \mathbb{Z}_n : \text{mcd}(r,n) = 1\}$. En $\mathbb{U}_n$ se define $[a]_n \cdot_n [b]_n = [ab]_n$. Se verifica que $(\mathbb{U}_n, \cdot_n)$ es un grupo abeliano, que se denomina **grupo de unidades** módulo n

Grupos $(\mathbb{Q}, +)$ y $(\mathbb{Q}^*, \cdot)$

En el conjunto $\mathbb{Z} \times \mathbb{N}$ se define la relación de equivalencia R_q: $(a,n) \sim_{\mathbb{Q}} (b,m) \Leftrightarrow am = bn$.
El conjunto cociente es: $\mathbb{Q} = (\mathbb{Z} \times \mathbb{N})/\sim_{\mathbb{Q}}$. Cada clase $[(a,n)] = \{(b,m) \in \mathbb{Z} \times \mathbb{N} : am = bn\} \in \mathbb{Q}$ se escribe: $[(a,n)] = \frac{a}{n} \in \mathbb{Q}$; si $n = 1$ se suele escribir simplemente: $[(a,1)] = \frac{a}{1} = a \in \mathbb{Q}$.

1. En $\mathbb{Q}$ se define la operación suma $\frac{a}{n} + \frac{b}{m} = \frac{ma+nb}{mn}$. Se verifica que $(\mathbb{Q}, +)$ es grupo abeliano
2. Sea $\mathbb{Q}^* = \mathbb{Q} - \{0\}$. En $\mathbb{Q}^*$ se define $\frac{a}{n} \cdot \frac{b}{m} = \frac{ab}{mn}$. Se verifica que $(\mathbb{Q}^*, \cdot)$ es grupo abeliano

Producto directo de grupos

Sean $(G_1, *_1)$ y $(G_2, *_2)$ dos grupos. En el producto cartesiano $G_1 \times G_2$ se define la operación: para todo $(a_1, a_2), (b_1, b_2) \in G_1 \times G_2$, $(a_1, a_2) * (b_1, b_2) = (a_1 *_1 b_1,\ a_2 *_2 b_2) \Rightarrow (G_1 \times G_2, *)$ es un grupo que se llama **producto directo** de $(G_1, *_1)$ y $(G_2, *_2)$. Si tanto $(G_1, *_1)$ como $(G_2, *_2)$ son abelianos, el producto directo también lo es, en ese caso suele decirse **suma directa** y se escribe $G_1 \oplus G_2$.

Subgrupos

Sea $(G, *)$ un grupo y $H \subseteq G$. Se dice que H es **subgrupo** de $(G, *)$ si y sólo si $(H, *)$ es un grupo.
Para indicar que H es un subgrupo de $(G, *)$ se escribe $H \leq G$.
Un subgrupo $H \leq G$ se dice que es **subgrupo propio** de $(G, *)$ si $H \subset G$ y $H \neq G$. Se escribe $H < G$.
Sea e_G el elemento neutro de $(G, *)$, entonces $H_0 = \{e_G\} \leq G$ y se denomina **subgrupo trivial**.

Definición equivalente de subgrupo

Sea $(G, *)$ un grupo y $H \subseteq G$, entonces H es **subgrupo** de $(G, *)$ si y sólo si:

- $e_G \in H$, siendo $e_G \in G$ el elemento neutro del grupo $(G, *)$.
- La operación $*$ es interna en H: Para todos $a, b \in H$ se verifica que $a * b \in H$.
- Para todo $a \in H$ se verifica que $a^{-1} \in H$, siendo $a^{-1} \in G$ el inverso de a en G.

Caracterización de subgrupo

Si $(G, *)$ es un grupo y $\emptyset \neq H \subseteq G$ entonces $H \leq G \Leftrightarrow \forall\ a, b \in H$ se verifica que $a * b^{-1} \in H$

1.1. Problemas

1. Las propiedades que debe cumplir un par $(G, *)$ para ser grupo, se han enunciado en el siguiente orden: g_1, g_2, g_3. Otros posibles órdenes para enunciarlos son: g_1, g_3, g_2; g_2, g_1, g_3; g_2, g_3, g_1; g_3, g_1, g_2 y g_3, g_2, g_1. De estos 6 órdenes posibles exactamente 3 son aceptables para una definición ¿Qué órdenes no son aceptables y por qué? g_2 no puede ir delante de g_1

2. Probar que la tabla de Cayley de todo grupo finito forma una distribución en la que cada elemento del grupo aparece una y sólo una vez en cada fila y cada columna (tal distribución se la denomina **Cuadrado Latino**). ¿Es todo cuadrado latino la tabla de un grupo?

3. Proceder del siguiente modo para mostrar que hay esencialmente dos grupos diferentes de orden 4. Concluir si es cierto que todo grupo de orden 4 es abeliano.

Si $G = \{e, a, b, c\}$ es un grupo y e es el elemento neutro, la tabla del grupo será:

$*$	e	a	b	c
e	e	a	b	c
a	a	?		
b	b			
c	c			

El cuadro marcado con ? puede contener e, b y c.

   a) Si en el cuadro se escribe e la tabla puede completarse de dos maneras para dar grupo. Encontrar estas dos tablas. (No es necesario corroborar la propiedad asociativa)

   b) Si en el cuadro se escribe b entonces se puede completar la tabla de un solo modo para dar grupo. Encontrar dicha tabla. (Tampoco aquí es necesario corroborar la propiedad asociativa)

   c) Si en el cuadro se escribe c entonces se puede completar la tabla de un solo modo para dar grupo. Encontrar dicha tabla. (No es necesario corroborar la propiedad asociativa)

   d) De las tablas obtenidas, sólo hay dos estructuras de grupo distintas. Determinar cuáles son y mostrar la manera de cambiar los nombres de los elementos para ver la coincidencia de tablas.

4. Demostrar que en todo grupo $(G, \cdot)$ se verifica que: $(a^{-1})^{-1} = a$ para todo $a \in G$

5. Demostrar que si $(G, \cdot)$ es un grupo y $a, b \in G$ entonces $(ab)^{-1} = b^{-1}a^{-1}$

6. Sean a y b elementos de un grupo $(G, \cdot)$. Demostrar que $ab^n a^{-1} = (aba^{-1})^n$.

7. Demostrar que si $(G, \cdot)$ es un grupo con elemento neutro $e \in G$ y tal que para todo $a \in G$ se verifica que $a^2 = e$, entonces $(G, \cdot)$ es abeliano.

8. Demostrar que si $(G, \cdot)$ es un grupo en el que para todo par de elementos $a, b \in G$ se verifica que $(ab)^2 = a^2b^2$ entonces $(G, \cdot)$ es abeliano.

9. Demostrar que si $(G, \cdot)$ es un grupo finito de orden par entonces existe un elemento $a \in G$ distinto del neutro, que verifica que $a^2 = e$.

10. Estudiar en cada caso si la operación $*$ dota al conjunto correspondiente de estructura de grupo. En caso afirmativo obtener el elemento neutro, el inverso de cada elemento e indicar si el grupo es abeliano.

   a) En $\mathbb{Z}$, $a * b = a - b$.

   b) En $G = \{2n+1 : n \in \mathbb{Z}\}$ se define $*$ por: $a * b = a + b$

   c) En $G = \mathbb{R} - \{-1\}$, $a * b = a + b + ab$.

   d) $H = \{\begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix} : x, y, z \in \mathbb{R}\}$ con la operación:

   $$\begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & x' & y' \\ 0 & 1 & z' \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x+x' & y+y'+xz' \\ 0 & 1 & z+z' \\ 0 & 0 & 1 \end{pmatrix}$$ (**Grupo de Heisenberg**).

11. Determinar cuales de los siguientes subconjuntos de $\mathbb{R}$ son subgrupos de $(\mathbb{R}, +)$:

   a) $\mathbb{Q}^+ = \{\frac{p}{q} \in \mathbb{Q} : \frac{p}{q} > 0\}$

   b) $7\mathbb{Z} = \{7n : n \in \mathbb{Z}\}$

   c) $\pi\mathbb{Q} = \{\pi q : q \in \mathbb{Q}\}$

   d) $\{\pi^n : n \in \mathbb{Z}\}$

12. Demostrar que si H y K son subgrupos de un grupo abeliano $(G, *)$ entonces también es subgrupo de $(G, *)$ el conjunto $HK = \{h * k : h \in H, k \in K\}$

13. Sea $(G, *)$ un grupo y $a \in G$, se llama **centralizador de** a al subconjunto $C(a) = \{g \in G : g * a = a * g\}$ (elementos de G que conmutan con a). Demostrar que $C(a)$ es un subgrupo de G.

14. Sea $(G, *)$ un grupo, el conjunto $Z(G) = \{g \in G : x * g = g * x$ para todo $x \in G\}$ se denomina **centro de** G. Demostrar las siguientes proposiciones:

   a) $Z(G) \leq G$. b) $Z(G) = \bigcap_{a \in G} C(a)$. c) $a \in Z(G) \Leftrightarrow C(a) = G$

15. Sea $G = \{T_{a,b} : \mathbb{R} \to \mathbb{R}$, $a, b \in \mathbb{R}$ con $a \neq 0$, aplicaciones definidas por $T_{a,b}(r) = ar + b\}$. Se considera en G la operación composición de funciones.

   a) Demostrar que $(G, \circ)$ es un grupo. ¿Es grupo abeliano?

   b) Demostrar que $H = \{T_{a,b} \in G : a \in \mathbb{Q}\}$ es un subgrupo de G, ¿es $(H, \circ)$ abeliano?

   c) Demostrar que $K = \{T_{a,b} \in G : a = 1\}$ es un subgrupo de G, ¿es $(K, \circ)$ abeliano?

   d) Sea $T_{a,b} \in G$ con $a \neq 1$, calcular el subgrupo $C(T_{a,b}) = \{U \in G : U * T_{a,b} = T_{a,b} * U\}$.

1.2. Generadores. Grupos cíclicos, diédricos y cuaterniones

Sistemas de generadores

Sean $(G,*)$ un grupo y $A \subseteq G$ un subconjunto no vacío de G.
El menor subgrupo de $(G,*)$ que contiene a A se denomina el **subgrupo generado por** A:

$$\langle A \rangle = \{a_1^{r_1} * \ldots * a_n^{r_n} : \text{ donde } a_i \in A, r_i \in \mathbb{Z}, \text{ y } n \in \mathbb{N}\}$$

- Un conjunto $A \subseteq G$ es un **sistema de generadores** del grupo $(G,*)$ si verifica que $G = \langle A \rangle$.
- El grupo $(G,*)$ es **cíclico** si tiene un sistema de generadores con un único elemento: existe $g \in G$ tal que $G = \langle g \rangle = \{g^n : n \in \mathbb{Z}\}$, en notación aditiva: $G = \langle g \rangle = \{ng : n \in \mathbb{Z}\}$.

Orden de un elemento

Sean $(G,*)$ un grupo y $a \in G$.
Se llama **orden de** a al menor entero positivo $r \in \mathbb{Z}^+$ tal que $a^r = e_G$. Se escribe $|a|_* = r$.
Si para todo $n \in \mathbb{Z}^+$ se verifica que $a^n \neq e_G$, se dice que el orden de a es infinito y se escribe $|a|_* = \infty$.

Orden de un elementos y orden del subgrupo que genera

Sean $(G,*)$ un grupo y $a \in G$. El orden de a coincide con el orden del subgrupo cíclico que genera:

$$|a|_* = |\langle a \rangle|$$

Orden de elementos de un grupo cíclico

Sea $(G,*)$ un grupo cíclico de orden n, y sea $g \in G$ un generador de G

1. Para todo $k \in \mathbb{Z}$, se verifica que $g^k = e_G \Leftrightarrow n$ divide a k
2. El orden de $g^k \in G$ es: $|g^k|_* = \frac{n}{\text{mcd}(k,n)}$.

Propiedades de grupos cíclicos

1. Todo grupo cíclico es abeliano.
2. Todo subgrupo de un grupo cíclico es cíclico.

Grupo de cuaterniones y grupos diédricos

- Se llama **grupo de cuaterniones** Q_8 al grupo generado por dos elementos de orden 4, $a, b \in Q_8$ tales que $ba = a^{-1}b$ y $b^2 = a^2$.

$$Q_8 = \langle a, b : |a| = 4, b^2 = a^2, ba = a^{-1}b \rangle$$

- Para todo $n > 2$, se llama **grupo diédrico** D_n al grupo de las simetrías de un polígono regular de n lados. Su orden es $2n$ y está generado por un elemento $a \in D_n$ de orden n y un elemento $b \in D_n$ de orden 2 tales que $ba = a^{-1}b$.

$$D_n = \langle a, b : |a| = n, |b| = 2, ba = a^{-1}b \rangle$$

Por analogía se define $D_2 = \langle a, b : |a| = 2, |b| = 2, ba = a^{-1}b \rangle$, que también recibe el nombre de **grupo cuatro de Klein**

Grupo cuatro de Klein $D_2 = \langle a, b : |a| = |b| = 2, ba = ab \rangle$

$*$	e	a	b	ab
e	e	a	b	ab
a	a	e	ab	b
b	b	ab	e	a
ab	ab	b	a	e

$$\langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \rangle$$

Grupo $D_4 = \langle a, b : |a| = 4, |b| = 2, ba = a^{-1}b \rangle$

$*$	e	a	a^2	a^3	b	ab	a^2b	a^3b
e	e	a	a^2	a^3	b	ab	a^2b	a^3b
a	a	a^2	a^3	e	ab	a^2b	a^3b	b
a^2	a^2	a^3	e	a	a^2b	a^3b	b	ab
a^3	a^3	e	a	a^2	a^3b	b	ab	a^2b
b	b	a^3b	a^2b	ab	e	a^3	a^2	a
ab	ab	b	a^3b	a^2b	a	e	a^3	a^2
a^2b	a^2b	ab	b	a^3b	a^2	a	e	a^3
a^3b	a^3b	a^2b	ab	b	a^3	a^2	a	e

$$\langle \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \rangle$$

Grupo $Q_8 = \langle a, b : |a| = 4, b^2 = a^2, ba = a^{-1}b \rangle$

$*$	e	a	a^2	a^3	b	ab	a^2b	a^3b
e	e	a	a^2	a^3	b	ab	a^2b	a^3b
a	a	a^2	a^3	e	ab	a^2b	a^3b	b
a^2	a^2	a^3	e	a	a^2b	a^3b	b	ab
a^3	a^3	e	a	a^2	a^3b	b	ab	a^2b
b	b	a^3b	a^2b	ab	a^2	a	e	a^3
ab	ab	b	a^3b	a^2b	a^3	a^2	a	e
a^2b	a^2b	ab	b	a^3b	e	a^3	a^2	a
a^3b	a^3b	a^2b	ab	b	a	e	a^3	a^2

$$\langle \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \rangle$$

Grupo $W_8 = \langle a, b : |a| = 4, |b| = 2, ba = ab \rangle$

$*$	e	a	a^2	a^3	b	ab	a^2b	a^3b
e	e	a	a^2	a^3	b	ab	a^2b	a^3b
a	a	a^2	a^3	e	ab	a^2b	a^3b	b
a^2	a^2	a^3	e	a	a^2b	a^3b	b	ab
a^3	a^3	e	a	a^2	a^3b	b	ab	a^2b
b	b	ab	a^2b	a^3b	e	a	a^2	a^3
ab	ab	a^2b	a^3b	b	a	a^2	a^3	e
a^2b	a^2b	a^3b	b	ab	a^2	a^3	e	a
a^3b	a^3b	b	ab	a^2b	a^3	e	a	a^2

$$\langle \begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \rangle$$

Diagrama de Cayley de un grupo

Sea $(G, *)$ un grupo finito de orden n, con generadores $\{g_1, ..., g_r\}$. $(G, *)$ puede representarse gráficamente mediante un digrafo de n vértices, donde cada vértice representa un elemento de G, y existe un arco etiquetado con un generador g_k, que va del vértice a_i al vértice $a_j \Leftrightarrow g_k * a_i = a_j$

1.2. Problemas

1. Dado un grupo $(G, *)$, demostrar que para todos $a, b, g \in G$ se verifica:
   a) $|a|_* = |a^{-1}|_*$
   b) $|a|_* = |g^{-1}ag|_*$
   c) $|ab|_* = |ba|_*$
2. Qué orden puede tener el elemento $a \in G$ si $a^{24} = e$.
3. Sea $(G, *)$ un grupo y sean $a, b \in G$ tales que $b \neq e$. Si $|a|_* = 2$ y $b^2 = aba$ ¿qué puede decirse sobre el orden de b?
4. Sea $(G, *)$ un grupo y sean $a, b \in G$ tales que $b \neq e$
   a) Demostrar que si $aba^{-1} = b^k$ entonces $a^r ba^{-r} = b^{k^r}$
   b) Si $|a|_* = 5$ y $b^2 = aba^{-1}$ ¿qué puede decirse sobre el orden de b?
5. Escribir al menos 5 elementos de cada uno de los siguientes subgrupos cíclicos:
   a) $\langle 25 \rangle \leq (\mathbb{Z}, +)$
   b) $\langle \frac{1}{2} \rangle \leq (\mathbb{Q}^*, \cdot)$
   c) $\langle \pi \rangle \leq (\mathbb{R}^*, \cdot)$
6. Indicar cuáles de los siguientes grupos son cíclicos y obtener sus generadores.
   $(H_1, *_1) = (\mathbb{Z}, +)$ $(H_2, *_2) = (\mathbb{Q}, +)$ $(H_3, *_3) = (\mathbb{Q}^* = \mathbb{Q} - \{0\}, \cdot)$ $(H_4, *_4) = (6\mathbb{Z}, +)$
   $(H_5, *_5) = (\{6^n : n \in \mathbb{Z}\}, \cdot)$ $(H_6, *_6) = (\{a + b\sqrt{2} : a, b \in \mathbb{Z}\}, +)$
7. Encontrar un generador de cada uno de los siguientes subgrupos de $(\mathbb{Z}_{12}, +_{12})$:
   a) $\langle 2, 3 \rangle$ b) $\langle 4, 6 \rangle$ c) $\langle 6, 8, 10 \rangle$
8. Se considera el grupo $G = \langle g \rangle = \{e = g^6, a_1 = g, a_2 = g^2, a_3 = g^3, a_4 = g^4, a_5 = g^5\}$. Calcular los subgrupos $\langle a_2 \rangle$, $\langle a_3 \rangle$, $\langle a_4 \rangle$, $\langle a_5 \rangle$. ¿Cuáles son los generadores de G?
9. Obtener el orden de cada uno de los elementos del grupo $(\mathbb{Z}_2 \times \mathbb{Z}_4, +)$ y encontrar un generador en caso de que fuera cíclico o un conjunto generador en caso de no ser cíclico.
10. Encontrar el número de generadores de los grupos cíclicos de órdenes 6, 8, 12 y 60.
11. Demostrar que si $(G, *)$ es un grupo que no tiene subgrupos propios no triviales, entonces es cíclico.
12. Demostrar que si $(G, *)$ es un grupo que no tiene subgrupos propios no triviales, entonces su orden es primo.

13. Encontrar el número de elementos de cada uno de los subgrupos cíclicos indicados:

    a) $H_a = \langle 25 \rangle \leq \mathbb{Z}_{30}$

    b) $H_b = \langle 30 \rangle \leq \mathbb{Z}_{42}$

    c) $H_c = \langle i \rangle \leq \mathbb{C}^* = \mathbb{C} - \{0\}$

    d) $H_d = \langle \frac{1+i}{\sqrt{2}} \rangle \leq \mathbb{C}^* = \mathbb{C} - \{0\}$

    e) $H_e = \langle i + 1 \rangle \leq \mathbb{C}^* = \mathbb{C} - \{0\}$

14. Sea $n \in \mathbb{N}$, demostrar que para todo k divisor n, el grupo $(\mathbb{Z}_n, +_n)$ tiene un único subgrupo de orden k, que es $H_k = \langle \frac{n}{k} \rangle$.

15. Sea H un subgrupo propio de $(\mathbb{Z}, +)$. Estudiar si puede determinarse el subgrupo H en cada uno de los siguientes casos:

    a) Si $18, 30, 40 \in H$

    b) Si $12, 30, 54 \in H$

16. Dibujar el diagrama de Cayley de los grupos D_2, D_4, Q_8 y W_8.

17. Demostrar que se cumple que $Y^2 = J^2 = K^2 = -q_0$, $YJ = K$, $JK = Y$, $KY = J$, $JY = -K$, $KJ = -Y$, y $YK = -J$. Obtener el orden de cada elemento y un conjunto generador del grupo $(\mathcal{Q}, \cdot)$. $\mathcal{Q} = \{q_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, Y = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, J = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, K = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix},$
    $-q_0 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, -Y = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, -J = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}, -K = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}\}$.

18. Describir el grupo de simetrías de un rectángulo y encontrar un conjunto generador.

19. Describir el grupo de simetrías de un rombo y encontrar un conjunto generador.

20. Se considera el grupo diédrico $(D_n, \circ)$, $D_n = \langle a, b : |a| = n, b^2 = e, ba = a^{-1}b \rangle$.

    a) Demostrar que $ba^r = a^{-r}b$ para todo $0 \leq r < n$

    b) Demostrar que todo elemento de la forma $a^r b$ tiene orden 2

    c) Encontrar el centro de D_n

21. Encontrar en cada caso, un grupo con las condiciones requeridas:

    a) G contiene elementos a y b tales que $|a| = |b| = 2$ y $|ab| = 3$

    b) G contiene elementos a y b tales que $|a| = |b| = 2$ y $|ab| = 4$

    c) G contiene elementos a y b tales que $|a| = |b| = 2$ y $|ab| = 5$

22. Demostrar que D_6 tiene un subgrupo de orden 4

23. Demostrar que D_3 no tiene un subgrupo de orden 4

1.3. Grupos de permutaciones

Sea X un conjunto no vacío, se nota por $(S_X, \circ)$ al **grupo de las aplicaciones biyectivas en X** con la operación composición de aplicaciones. En particular si $X = \{1, 2, 3, ..., n\}$ el grupo se nota por $(S_n, \circ)$, se denomina **grupo simétrico** y cada uno de sus elementos recibe el nombre de **permutación**. Se llama **grupo de permutaciones** a todo subgrupo del grupo simétrico $(S_n, \circ)$.

Sea $\sigma \in S_n$, se dice que σ es un **ciclo** de longitud r si existen $a_0, \cdots, a_{r-1} \in \{1, \cdots, n\}$ tales que $\sigma(a_0) = a_1$, $\sigma(a_1) = a_2$, $\cdots$, $\sigma(a_{r-2}) = a_{r-1}$, $\sigma(a_{r-1}) = a_0$, y para todo $k \in \{1, \cdots, n\}$ tal que $k \notin \{a_0, \cdots, a_{r-1}\}$ se verifica que $\sigma(k) = k$. La notación de dicho ciclo es $\sigma = (a_0, a_2, \cdots, a_{r-1})$.

Dos ciclos $\sigma \in S_n$ y $\tau \in S_n$ se dice que son **disjuntos** si ninguno de los elementos del conjunto $\{1, 2, ..., n\}$ aparece en la notación de ambos. Los ciclos de longitud 2 se denominan **transposiciones**.

$\beta\alpha(1) = \beta(\alpha(1)) = \beta(2) = 5$

Propiedades

1. Los ciclos disjuntos conmutan: Si $\sigma, \tau \in S_n$ son dos ciclos disjuntos entonces $\sigma\tau = \tau\sigma$.
2. El orden de un ciclo es su longitud

Formas de expresar una permutación

1. Toda permutación $\sigma \in S_n$ se puede expresar como **producto de ciclos disjuntos**.
2. Toda permutación $\sigma \in S_n$, con $n \geq 2$, se puede expresar como **producto de transposiciones**.

Lema 1. Reordenación de componentes en transposiciones

Dado un producto de $r > 0$ transposiciones: $\tau_1\tau_2...\tau_r$, siempre existe otro producto de transposiciones $\sigma_1\sigma_2...\sigma_s$ con $s \equiv r$ mód 2, $\tau_1\tau_2...\tau_r = \sigma_1\sigma_2...\sigma_s$, y verificando una de las siguientes condiciones:

- $s < r$ y la componente a de $\tau_r = (a, b)$ no aparece en ninguna transposición σ_i para $i \in \{1, ..., s\}$
- $s \leq r$ y la componente a de $\tau_r = (a, b)$ sólo aparece en la transposición σ_1.

Lema 2. La identidad como producto de transposiciones

La identidad de S_n, para $n \geq 2$, sólo puede descomponerse como producto de un número par de transposiciones.

Teorema. Paridad de una permutación

Si $\sigma \in S_n$ se puede expresar como producto de r transposiciones y como producto de s transposiciones entonces $r + s$ es par.

Definición. Permutaciones pares e impares

Una **permutación** de S_n es **par** o **impar** según pueda ser expresada como el producto de un número par o de un número impar de transposiciones respectivamente.

El grupo alternado A_n

Sea $n \geq 2$. El conjunto de todas las permutaciones pares de S_n es un subgrupo del grupo simétrico S_n que se denomina **grupo alternado** A_n y su orden es $\frac{n!}{2}$.

1.3. Problemas

1. Escribir cada una de las siguientes permutaciones como producto de ciclos disjuntos y como producto de transposiciones:

   a) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 6 & 4 & 1 & 8 & 2 & 5 & 7 \end{pmatrix}$ *b)* $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 5 & 7 & 8 & 4 & 6 & 1 & 2 & 9 \end{pmatrix}$

2. Escribir como producto de ciclos disjuntos: *a)* $\sigma\tau$, *b)* $\sigma\tau^2$, *c)* $\sigma^2\mu$, *d)* $\tau\sigma^{-2}$, *e)* $\sigma\tau\sigma^{-1}$, siendo $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 4 & 5 & 6 & 2 \end{pmatrix}$, $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 1 & 3 & 6 & 5 \end{pmatrix}$, $\mu = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 4 & 3 & 1 & 6 \end{pmatrix} \in S_6$

3. *a)* ¿Cuál es el orden del ciclo $(1,4,5,7) \in S_8$?

   b) ¿Cuál es el orden de $\sigma = (4,5)(2,3,7)$ y de $\tau = (1,4)(3,5,7,8)$ en S_8?

   c) Expresar como producto de ciclos disjuntos y obtener el orden: $\nu_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 2 & 6 & 3 & 7 & 4 & 5 & 1 \end{pmatrix}$,
   $\nu_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 6 & 4 & 1 & 8 & 2 & 5 & 7 \end{pmatrix}$, $\nu_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 1 & 4 & 7 & 2 & 5 & 8 & 6 \end{pmatrix}$, $\nu_4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 1 & 3 \end{pmatrix}$

4. Demostrar que A_8 contiene un elemento de orden 15

5. *a)* Sea $\beta = (1,3,5,7,9,8,6)(2,4,10)$. ¿Cuál es el menor entero positivo $n \in \mathbb{N}$ tal que $\beta^n = \beta^{-5}$

   b) Si $\alpha = (1,3,5,7,9)(2,4,6)(8,10)$ y α^m es ciclo de longitud 5 ¿qué puede decirse sobre m?

6. Se disponen 20 cartas numeradas en 5 filas de 4 columnas. En cada paso, se recogen las cartas en orden por filas y se vuelven a colocar en el mismo orden pero por columnas. ¿Cuántas veces hay que repetir este proceso hasta que las cartas aparezcan en la posición inicial?

7. ¿Cuales de los siguientes son subgrupos de S_5? $X_a = \{(1,2,3,4,5), (1,2,4)(3,5)\}$,
   $X_b = \{(1), (1,2,3,4,5), (1,3,5,2,4), (1,4,2,5,3), (1,5,4,3,2)\}$,
   $X_c = \{(1), (1,2)(3,4,5), (1,3,5)(2,4), (1,5,3,2,4), (1,2)(4,5), (1,3,4)(2,5), (1,4,3)(2,5)\}$.

8. Se considera el grupo $S_3 = \{\rho_0, \rho_1 = (1,2,3), \rho_2 = (1,3,2), \mu_1 = (2,3), \mu_2 = (1,3), \mu_3 = (1,2)\}$

   a) Encontrar los subgrupos cíclicos $\langle\rho_1\rangle$, $\langle\rho_2\rangle$ y $\langle\mu_1\rangle$ de S_3

   b) Encontrar todos los subgrupos de S_3 y elaborar con ellos un diagrama de Hasse.

   c) Encontrar las permutaciones pares y construir la tabla de A_3.

9. Encontrar los tres elementos $\alpha_1, \alpha_2, \alpha_3 \in S_4$ tales que, expresados en forma de producto de ciclos disjuntos, se componen de dos ciclos de longitud 2. Comprobar que $K = \{e, \alpha_1, \alpha_2, \alpha_3\}$ es un subgrupo de S_4 describiendo su tabla. Construir su diagrama de Cayley.

10. Sea $\tau = (a_0, a_1, ..., a_{k-1})$ un ciclo de longitud k

    a) Demostrar que para cualquier permutación σ, se verifica que $\sigma\tau\sigma^{-1} = (\sigma(a_0), \sigma(a_1), ..., \sigma(a_{k-1}))$

    b) Demostrar que para todo μ, ciclo de longitud k, existe σ tal que $\sigma\tau\sigma^{-1} = \mu$

11. Demostrar que una permutación es par si y sólo si puede expresarse como composición de 3−ciclos (no necesariamente disjuntos).

1.4. Isomorfismos en grupos

Dos grupos $(G, *_1)$ y $(G', *_2)$ son **isomorfos**, y se escribe $G \approx G'$, si existe una aplicación biyectiva $\phi : G \to G'$ tal que para todos $x, y \in G$ se verifica que

$$\phi(x *_1 y) = \phi(x) *_2 \phi(y)$$

La aplicación ϕ se denomina **isomorfismo de grupos**

Isomorfismos en grupos cíclicos

1. Todo grupo cíclico $(G, *)$ de orden infinito, es isomorfo a $(\mathbb{Z}, +)$
2. Todo grupo cíclico $(G, *)$ de orden n, es isomorfo a $(\mathbb{Z}_n, +_n)$

Producto de grupos cíclicos

El grupo $(\mathbb{Z}_m \times \mathbb{Z}_n, +_m \times +_n)$ es isomorfo a $(\mathbb{Z}_{mn}, +_{mn})$ si y sólo si $\text{mcd}(m, n) = 1$

Definición de producto directo interno

Sea $(G, *)$ un grupo y sean $H \leq G$ y $K \leq G$.
Se dice que el grupo G es **producto directo interno de los subgrupos** H y K si se verifica que:

1. $H \cap K = \{e\}$
2. $G = HK = \{h * k : h \in H, k \in K\}$
3. Los elementos de H y de K conmutan: $\forall\, h \in H, k \in K$ es $h * k = k * h$

Relación entre producto directo interno y producto directo

Si $(G, *)$ es producto directo interno de los subgrupos H y K entonces $G \approx H \times K$

Teorema de Cayley

Todo grupo de orden $n \in \mathbb{N}$ es isomorfo a un grupo de permutaciones.

1.4. Problemas

1. En el grupo $(S_4, \circ)$ sea $H = \{e = (1), a = (1,2)(3,4), b = (1,3)(2,4), c = (1,4)(2,3)\}$

   a) Demostrar, mediante la construcción de su tabla de Cayley, que H es abeliano.

   b) Estudiar si existe un isomorfismo de $(H, \circ)$ en $(\mathbb{Z}_2 \times \mathbb{Z}_2, +_2 \times +_2)$.

2. *a*) Estudiar si $(U_8, \cdot_8) \approx (\mathbb{Z}_4, +_4)$

   b) Estudiar si $(U_8, \cdot_8) \approx (M, \cdot)$, siendo $M = \{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}\}$, con el producto usual de matrices

3. Entre los grupos $(\mathbb{Z}_n, +_n)$, $(U_n, \cdot_n)$, $(D_n, \circ)$, $(S_n, \circ)$, $(\mathbb{Z}_n \times \mathbb{Z}_m, +_n \times +_m)$ y cuaterniones, encontrar uno isomorfo a $(V, \cdot)$, siendo $\cdot$ el producto usual de matrices y

$$V = \{\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}\}.$$

4. Estudiar si $(H = \{\begin{pmatrix} 1 & a & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} : a, b \in \mathbb{Z}_3\}, \cdot_3)$ es isomorfo a $(\mathbb{Z}_9, +_9)$ o a $(\mathbb{Z}_3 \times \mathbb{Z}_3, +_3 \times +_3)$

5. Demostrar que $G = \{\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} : a, b, c \in \mathbb{Z}_2\}$ con la operación producto de matrices, módulo 2, es isomorfo a D_4.

6. Estudiar si existe algún isomorfismo entre el grupo $(\mathbb{C}^*, \cdot)$ y el siguiente subgrupo de $GL_2(\mathbb{R})$:
   $C = \{\begin{pmatrix} a & b \\ -b & a \end{pmatrix} : a, b \in \mathbb{R}\} \leq GL_2(\mathbb{R})$

7. Se considera el grupo $(G = \mathbb{R} - \{-1\}, *)$, siendo $a * b = a + b + ab$. Demostrar que el grupo $(G, *)$ es isomorfo al grupo $(\mathbb{R}^*, \cdot)$

8. Probar que D_4 no puede ser producto directo interno de dos subgrupos propios.

9. Probar que D_6 es producto directo interno de dos de sus subgrupos propios.

2.1. Clases laterales. Teorema de Lagrange

Relación de equivalencia determinada por un subgrupo

Sea $(G, *)$ un grupo y H un subgrupo de G. La relación $a \sim_H b \Leftrightarrow a^{-1} * b \in H$ es una relación de equivalencia en G.

La clase de equivalencia de un elemento $a \in G$ se denomina **clase lateral izquierda** y es

$$[a]_H = aH = \{a * h : h \in H\}$$

Definición de índice

Sea H un subgrupo de $(G, *)$, se llama **índice de G sobre H** al número de clases laterales izquierdas de H en G y se nota por $[G : H]$

Teorema de Lagrange

Si $(G, *)$ es un grupo finito y $H \leq G$ entonces $|H|$ es un divisor de $|G|$ y se verifica que

$$\frac{|G|}{|H|} = [G : H]$$

Corolarios

1. Si $(G, *)$ es un grupo finito de orden primo entonces G es cíclico.
2. Si $(G, *)$ es un grupo finito con $|G| = n$ entonces para todo $a \in G$ es $a^n = e$.
3. Si H y K son subgrupos de $(G, *)$ tales que $K \subset H \subset G$ entonces $[G : K] = [G : H][H : K]$

Teorema de Fermat

Si $p \in \mathbb{N}$ es primo y $a \not\equiv 0$ mód p entonces $a^{p-1} \equiv 1$ mód p

Teorema de Euler

Si $\text{mcd}(a, m) = 1$ y φ es la función de Euler, entonces $a^{\varphi(m)} \equiv 1$ mód m

$$\varphi(m) = m \prod_{p \in \mathbb{N} \text{ divisor primo de } m} \left(1 - \frac{1}{p}\right)$$

Teorema de Cauchy

Sea $(G, *)$ un grupo de orden $n \in \mathbb{N}$.
Si $p \in \mathbb{N}$ es un divisor primo de $n \Rightarrow$ existe $a \in G$ tal que $|a|_* = p$

2.1. Problemas

1. En $(\mathbb{Z}, +)$ se considera el subgrupo $H = \{3n : n \in \mathbb{Z}\}$. Decidir cuales de los siguientes pares de clases laterales son las mismas

   a) $11 + H$ y $17 + H$

   b) $-1 + H$ y $5 + H$

   c) $7 + H$ y $23 + H$

2. Dados el grupo $(G, *)$ y $H \leq G$, calcular $|H|$ y $[G : H]$ en cada caso.

   a) $H = \langle [18]_{36} \rangle$, $(G, *) = (\mathbb{Z}_{36}, +_{36})$

   b) $H = \langle [3]_6 \rangle$, $(G, *) = (\mathbb{Z}_6, +_6)$

   c) $H = \langle [4]_{12} \rangle$, $(G, *) = (\mathbb{Z}_{12}, +_{12})$

   d) $H = \langle [12]_{60} \rangle$, $(G, *) = (\mathbb{Z}_{60}, +_{60})$

   e) $H = \langle [2]_4 \rangle \times \langle [2]_{12} \rangle$, $(G, *) = (\mathbb{Z}_4 \times \mathbb{Z}_{12}, +_4 \times +_{12})$

   f) $H = \langle ([2]_4, [2]_{12}) \rangle$, $(G, *) = (\mathbb{Z}_4 \times \mathbb{Z}_{12}, +_4 \times +_{12})$

   g) $H = \langle [1]_3 \rangle \times \langle [0]_2 \rangle \times \langle [0]_4 \rangle$, $(G, *) = (\mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_4, +_3 \times +_2 \times +_4)$

   h) $H = \langle [0]_3 \rangle \times \langle [1]_2 \rangle \times \langle [2]_4 \rangle$, $(G, *) = (\mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_4, +_3 \times +_2 \times +_4)$

3. Sean H y K dos subgrupos de un grupo $(G, \cdot)$ con $|G| = 660$. Si $|K| = 66$ y $K \subset H \subset G$ ¿qué orden puede tener el grupo H?

4. El grupo D_5 de las simetrías de un pentágono regular es un grupo de orden 10. Demostrar que tiene subgrupos de todos los órdenes permitidos por el teorema de Lagrange. Dar un esquema del retículo de sus subgrupos.

5. Sea $(G, *)$ un grupo y p un número primo. Demostrar que:

   a) Si G tiene orden $2p$ entonces todo subgrupo propio de G es cíclico

   b) Si G tiene orden p^2 entonces tiene un subgrupo de orden p. (Demostrar sin usar el teorema de Cauchy)

6. Sean H y K dos subgrupos de un grupo $(G, *)$.

   a) Demostrar que si $|H| = 10$ y $|K| = 21$ entonces $H \cap K = \{e\}$

   b) Demostrar que si $|H| = n$ y $|K| = m$ con $\text{mcd}(n, m) = 1$ entonces $H \cap K = \{e\}$

2.2. Subgrupos normales y grupos cocientes

Sea $(G, *)$ un grupo y $N \leq G$. La clase lateral izquierda de a es $[a]_N = aN = \{a * h : h \in N\}$. Se denomina **clase lateral derecha** de $a \in G$ al conjunto

$$Na = \{h * a : h \in N\}$$

El subgrupo $N \leq G$ se dice que es **normal** en G, y se escribe $N \trianglelefteq G$, si para todo $a \in G$ se verifica

$$[a]_N = aN = Na$$

Caracterización de subgrupos normales

Sea $(G, *)$ un grupo y $N \leq G$. Las siguientes proposiciones son equivalentes:

i) $aN = Na$ para todo $a \in G$

ii) $aNa^{-1} \subseteq N$ para todo $a \in G$

iii) $aNa^{-1} = N$ para todo $a \in G$

Los subgrupos de un grupo abeliano son normales

Si $(G, *)$ es un grupo abeliano y $H \leq G$, entonces $H \trianglelefteq G$

Los subgrupos de índice 2 son normales

Si $(G, *)$ es un grupo finito y $H \leq G$ tal que $[G : H] = 2$, entonces $H \trianglelefteq G$

Los subgrupos únicos en su orden son normales

Si $(G, *)$ es un grupo finito y $H \leq G$ es el único subgrupo de G cuyo orden es $|H|$ entonces $H \trianglelefteq G$

Teorema del grupo cociente

Sea $(G, *)$ un grupo y $N \trianglelefteq G$. Entonces $(G/N, *_N)$ es un grupo de orden $|G/N| = [G : N]$, siendo $G/N = \{gN : g \in G\}$ el conjunto de las clases laterales de N en G con la operación $aN *_N bN = (a*b)N$. Dicho grupo recibe el nombre de **grupo cociente** de G sobre N.

Definición de grupo simple

Un grupo $(G, *)$ se dice que es **simple** si no tiene subgrupos normales propios no triviales.

Observaciones

- Para todo $p \in \mathbb{N}$ primo, el grupo $(\mathbb{Z}_p, +_p)$ es simple
- Para todo $n \geq 5$, el grupo alternado $(A_n, \circ)$ es simple
- Si $(G, *)$ es un grupo y $N \trianglelefteq G$, se dice que N es un **subgrupo normal maximal** de $(G, *)$ si para todo $H \trianglelefteq G$ con $N \subseteq H$ se verifica que $N = H$ o $H = G$.
  En estas condiciones se tiene que:

  G/N es simple $\Leftrightarrow$ N es un subgrupo normal maximal de $(G, *)$

2.2. Problemas

1. Estudiar si H es un subgrupo normal de $(G, *)$ en cada caso:

   a) $H = \{(1), (1,2)\}$, $G = S_3$

   b) $H = \{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a, b, c \in \mathbb{R} \text{ tales que } ac \neq 0\}$, $G = GL_2(\mathbb{R})$

   c) $H = SL_2(\mathbb{R})$, $G = GL_2(\mathbb{R})$

   d) $H = A_4$, $G = S_4$

   e) $H = \{(1), (1,2,3), (1,3,2)\}$, $G = A_5$

   f) $H = D_4$, $G = S_4$

   g) $H = \{1, -1, i, -i\}$ en $Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$ grupo de los cuaterniones, que verifica: $(-1)^2 = 1$, $(-1)a = -a = a(-1)$ para todo $a \in Q_8$, $i^2 = j^2 = k^2 = -1$, $ij = -ji = k$, $jk = -kj = i$, $ki = -ik = j$

2. Sea $(G, *)$ un grupo, demostrar que $Z(G)$ es un subgrupo normal de G, siendo $Z(G)$ el centro de G: $Z(G) = \{g \in G : g * a = a * g \text{ para todo } a \in G\}$.

3. Sea $(G, *)$ un grupo y sea $H = \langle a * b * a^{-1} * b^{-1} : a, b \in G \rangle$. Demostrar que H es un subgrupo normal de G. H recibe el nombre de **subgrupo conmutador de** G. Demostrar que G/H es abeliano.

4. Dados el grupo $(G, *)$ y el subgrupo $H \leq G$, demostrar que $H \trianglelefteq G$, construir la tabla de Cayley del grupo cociente G/H y encontrar un grupo isomorfo a G/H.

   a) $(G, *) = (\mathbb{Z}, +)$ y $H = 5\mathbb{Z}$

   b) $(G, *) = (\mathbb{Z}_4 \times \mathbb{Z}_4, (+_4, +_4))$ y $H = \{([0]_4, [0]_4), ([2]_4, [0]_4), ([0]_4, [2]_4), ([2]_4, [2]_4)\}$

   c) $(G, *) = (\mathbb{Z}_4 \times \mathbb{Z}_4, (+_4, +_4))$ y $H = \langle([1]_4, [2]_4)\rangle$

   d) $(G, *) = (\mathbb{Z}_4 \times \mathbb{Z}_4^*, (+_4, \cdot_4))$ y $H = \langle([2]_4, [3]_4)\rangle$

   e) $(G, *) = (\mathbb{Z}_4 \times \mathbb{Z}_4^*, (+_4, \cdot_4))$ y $H = \langle([2]_4, [1]_4)\rangle$

   f) $(G, *) = (Q_8, \cdot)$ y $H = \{1, -1\}$

5. *a)* Encontrar todos los subgrupos de D_4 y estudiar cuales son normales.

   b) Calcular, salvo isomorfismos, todos los posibles grupos cocientes con el grupo D_4 y sus subgrupos normales.

6. Se considera el grupo $(\mathbb{R}, +)$ y el subgrupo $\mathbb{Z} \leq \mathbb{R}$.
   Demostrar que $\mathbb{Z} \trianglelefteq \mathbb{R}$ y obtener el grupo cociente $\mathbb{R}/\mathbb{Z}$.

2.3. Homomorfismos de grupos

Una aplicación $\varphi : G \to G'$ entre los grupos $(G, *)$ y $(G', \cdot)$ es un **homomorfismo de grupos** si para todos $x, y \in G$ se verifica que

$$\varphi(x * y) = \varphi(x) \cdot \varphi(y)$$

Si $\varphi : G \to G'$ es un homomorfismo de grupos, se llama **núcleo** de φ al conjunto

$$\ker(\varphi) = \{a \in G : \varphi(a) = e_{G'}\} = \varphi^{-1}(\{e_{G'}\})$$

Y se llama **imagen de** φ al conjunto

$$\varphi(G) = \{\varphi(a) : a \in G\}$$

Propiedades

Sean $(G, *)$ y $(G', \cdot)$ grupos y $\varphi : G \to G'$ homomorfismo. Se tiene que:

1. $\varphi(e_G) = e_{G'}$ siendo $e_G \in G$ y $e_{G'} \in G'$ los elementos neutros de $(G, *)$ y $(G', \cdot)$ respectivamente
2. $\varphi(a)^{-1} = \varphi(a^{-1})$ para todo $a \in G$
3. φ es inyectivo $\Leftrightarrow \ker(\varphi) = \{e_G\}$
4. φ es suprayectivo $\Leftrightarrow \varphi(G) = G'$

Subgrupo núcleo y subgrupo imagen

Si $\varphi : G \to G'$ es un homomorfismo de grupos entonces:

1. $\ker(\varphi) \trianglelefteq G$
2. $\varphi(G) \leq G'$

Primer teorema de Isomorfía

Sea $\varphi : G \to G'$ un homomorfismo de grupos, entonces

$$G/\ker(\varphi) \approx \varphi(G)$$

Corolario 1

Si $(G, *)$ y $(G', \cdot)$ son dos grupos finitos y $\varphi : G \to G'$ es un homomorfismo de grupos entonces:

$$|\varphi(G)| \quad \text{divide a} \quad |G'| \quad \text{y también divide a} \quad |G|$$

Corolario 2

La aplicación $\varphi : \mathbb{Z}_n \to \mathbb{Z}_m$ es un homomorfismo entre los grupos $(\mathbb{Z}_n, +_n)$ y $(\mathbb{Z}_m, +_m)$ si y sólo si

$$\varphi([a]_n) = [ak]_m \quad \text{siendo} \quad nk \equiv 0 \mod m$$

2.3. Problemas

1. Estudiar si son homomorfismos de grupos y en caso afirmativo encontrar el núcleo, la imagen y establecer el isomorfismo dado por el primer teorema de isomorfía.

   a) $\varphi : \mathbb{R}^* \to GL_2(\mathbb{R})$, $\varphi(a) = \begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix}$

   b) $\varphi : \mathbb{R} \to GL_2(\mathbb{R})$, $\varphi(a) = \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}$

   c) $\varphi : GL_2(\mathbb{R}) \to \mathbb{R}$, $\varphi(\begin{pmatrix} a & b \\ c & d \end{pmatrix}) = a + d$

   d) $\varphi : GL_2(\mathbb{R}) \to \mathbb{R}^*$, $\varphi(\begin{pmatrix} a & b \\ c & d \end{pmatrix}) = ad - bc$

   e) $\varphi : \mathbb{Z} \to \mathbb{Z}$, $\varphi(n) = 7n$

2. Sea $\varphi : \mathbb{Z}_{30} \to \mathbb{Z}_{30}$ un homomorfismo cuyo núcleo es $\ker(\varphi) = \{[0]_{30}, [10]_{30}, [20]_{30}\}$. Si $\varphi([23]_{30}) = [9]_{30}$ determinar todos los elementos que se transforman en $[9]_{30}$

3. Sea $\varphi : \mathbb{Z}_{30} \to G$ un homomorfismo suprayectivo de grupos. Sabiendo que $|G| = 5$, calcular $\ker(\varphi)$

4. Sea $\varphi : \mathbb{Z}_{17} \to G$ un homomorfismo de grupos que no es inyectivo. Determinar φ

5. ¿Cuántos homomorfismo existen de $(\mathbb{Z}_{20}, +_{20})$ en $(\mathbb{Z}_8, +_8)$?, ¿cuántos de ellos son suprayectivos?

6. Sean $(G, *)$ y $(G', \cdot)$ dos grupos de órdenes 24 y 7 respectivamente. Estudiar si existe un homomorfismo suprayectivo de G en G' y si existe un homomorfismo inyectivo de G' en G.

7. Estudiar si existe algún homomorfismo inyectivo $\varphi : D_4 \to \mathbb{Z}_{16}$

8. Describir los homomorfismos $\varphi : \mathbb{Z}_{24} \to \mathbb{Z}_{18}$

9. Construir un homomorfismo de grupos cuyo núcleo sea isomorfo a $\mathbb{Z}_3$, otro con núcleo isomorfo a $\mathbb{Z}_4$ y otro con núcleo isomorfo a $\mathbb{Z}_6$.

2.4. Estructura de grupos

Definición de $p-$grupos

Sea $(G,*)$ un grupo finito y $p \in \mathbb{N}$ un número primo.

- Un subgrupo $H \leq G$ se dice que es un $p-$**grupo** o $p-$**subgrupo** de $G \Leftrightarrow$ $|H|$ es potencia de p.
- Un subgrupo $H \leq G$ se dice que es un $p-$**grupo de Sylow** de $G \Leftrightarrow$ H es un $p-$subgrupo y su orden coincide con la máxima potencia de p que divide a $|G|$.

Teoremas de Sylow

1. **Existencia de $p-$grupos**
   Si $(G,*)$ es un grupo finito y p^n es la mayor potencia de $p \in \mathbb{N}$ primo que divide a $|G| \Rightarrow$ hay $p-$subgrupos de G de órdenes $1, p, p^2, \cdots, p^n$ y todo $p-$subgrupo está contenido en un $p-$grupo de Sylow de G.

2. **Relación entre $p-$grupos de Sylow**
   Si H y K son dos $p-$subgrupos de Sylow de G entonces existe $g \in G$ tal que
   $$H = gKg^{-1}$$

3. **El número de $p-$grupos de Sylow**
   Sea $p \in \mathbb{N}$ un número primo tal que $p \,||G|$.
   El número n de $p-$subgrupos de Sylow de G verifica lo siguiente:
   $$n \text{ divide a } |G| \quad \text{y} \quad n \equiv 1 \mod p$$

Observaciones

1. Sea S_p un $p-$grupo de Sylow de $(G,*)$. S_p es el único $\Leftrightarrow H \trianglelefteq G$
2. Todo grupo **abeliano finito** es isomorfo al producto directo de sus $p-$grupos de Sylow:
   Si $(G,*)$ es un grupo abeliano con $|G| = p^t m$, $p \in \mathbb{N}$ primo y $\text{mcd}(p,m) = 1 \Rightarrow$ $G \approx S_p \times K$ siendo: $S_p = \{x \in G : x^{p^t} = e_G\}$ y $K = \{x \in G : x^m = e_G\}$
3. Si $a \in S_p$ es un elemento de orden máximo en $S_p \Rightarrow$ existe $H \leq S_p$ tal que
   $$S_p \approx \langle a \rangle \times H$$

Teorema de estructura de grupos abelianos finitos

Todo grupo abeliano finito es isomorfo a un producto directo de grupos cíclicos de la forma

$$\mathbb{Z}_{q_1^{\beta_1}} \times \mathbb{Z}_{q_2^{\beta_2}} \times \cdots \times \mathbb{Z}_{q_r^{\beta_r}}$$

donde $q_1 \leq q_2 \leq \cdots \leq q_r$ son primos no necesariamente distintos.

Divisores elementales y Factores invariantes de grupos abelianos finitos

Sea $(G,*)$ un grupo abeliano finito, entonces:

1. Si $G \approx \mathbb{Z}_{q_1^{\beta_1}} \times \mathbb{Z}_{q_2^{\beta_2}} \times \cdots \times \mathbb{Z}_{q_r^{\beta_r}}$ con $q_1 \leq q_2 \leq \cdots \leq q_r$ números primos no necesariamente distintos, los enteros $q_1^{\beta_1}, q_2^{\beta_2}, \cdots, q_r^{\beta_r}$ reciben el nombre de **divisores elementales** del grupo.
2. Si $G \approx \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_k}$ con $m_1 \geq m_2 \geq \ldots \geq m_k \geq 1$ verificando que para $i \in \{1, \cdots, k-1\}$ $m_{i+1} | m_i$, los enteros $m_1, m_2, \cdots, m_k$ reciben el nombre de **factores invariantes** del grupo.

2.4. Problemas

1. Señalar cuales de los siguientes grupos son cíclicos:
   a) $\mathbb{Z}_6 \times \mathbb{Z}_5$
   b) $\mathbb{Z}_7 \times \mathbb{Z}_6 \times \mathbb{Z}_4$
   c) $\mathbb{Z}_3 \times \mathbb{Z}_{25} \times \mathbb{Z}_2$
   d) $\mathbb{Z}_6 \times \mathbb{Z}_{15} \times \mathbb{Z}_2$
2. Determinar salvo isomorfismos, todos los grupos abelianos de orden n:
   a) $1 < n < 20$
   b) $n = 64$
   c) $n = 360$
   d) $n = 96$
   e) $n = 720$
   f) $n = 1089$
3. ¿Es $\mathbb{Z}_{54} \times \mathbb{Z}_{12} \times \mathbb{Z}_{72}$ isomorfo a $\mathbb{Z}_{48} \times \mathbb{Z}_{27} \times \mathbb{Z}_{36}$?
4. ¿Qué grupos abelianos de orden 360 tienen un elemento de orden 30?
5. Demostrar que cualquier grupo abeliano de orden 36 tiene elementos de orden 6 ¿y de orden 9?
6. Si $(G, *)$ es un grupo abeliano de orden 100 demostrar que contiene un elemento de orden 10.
7. ¿Cuántos subgrupos de orden 11 tiene un grupo abeliano de orden 33?
8. Se consideran 6 grupos abelianos de orden 16. Demostrar que al menos dos de ellos son isomorfos.
9. Demostrar que $\mathbb{Z}_{10} \approx H \times K$ siendo $H = \{[0]_{10}, [5]_{10}\} \leq \mathbb{Z}_{10}$ y $K = \{[0]_{10}, [2]_{10}, [4]_{10}, [6]_{10}, [8]_{10}\} \leq \mathbb{Z}_{10}$
10. Demostrar que el grupo multiplicativo $(U_{21}, \cdot_{21})$ es isomorfo a un producto directo de los subgrupos $H = \langle [2]_{21} \rangle$ y $K = \langle [13]_{21} \rangle$.
11. Encontrar los factores invariantes:
    a) $\mathbb{Z}_5 \times \mathbb{Z}_{15} \times \mathbb{Z}_{25} \times \mathbb{Z}_{36}$
    b) $\mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_{35}$
    c) $\mathbb{Z}_{26} \times \mathbb{Z}_{42} \times \mathbb{Z}_{49} \times \mathbb{Z}_{200} \times \mathbb{Z}_{100}$
    d) $\mathbb{Z}_{20} \times \mathbb{Z}_6 \times \mathbb{Z}_4 \times \mathbb{Z}_{18} \times \mathbb{Z}_{12} \times \mathbb{Z}_{10}$
    e) $(U_{20}, \cdot_{20})$
    f) $(U_{22}, \cdot_{22})$
    g) $(\mathbb{Z}_{20} \times \mathbb{Z}_5)/\langle([0]_{20}, [1]_5)\rangle$
    h) $(\mathbb{Z}_6 \times \mathbb{Z}_8)/\langle([1]_6, [2]_8)\rangle$
    i) $(\mathbb{Z}_3 \times \mathbb{Z}_4 \times \mathbb{Z}_6)/\langle([1]_3, [1]_4, [1]_6)\rangle$
    j) $(\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_3)/(\langle[2]_4\rangle \times \langle[0]_2\rangle \times \langle[1]_3\rangle)$